Amendments to the Specification:

Please replace the Abstract with the following amended Abstract:

ABSTRACT

In the event of cryptographically processing data, ~~said~~ data (X) and a key (K) are fed to a cryptographic process (P), which may be a known process. In order to veil the nature of the process (P), there are fed auxiliary values to the process, such as a supplementary key (K*), using which a supplementary process (P*) generates the key proper (K). The combination of the original process (P) and the supplementary process (P*) provides an unknown process, the relationship between the supplementary key (K*) and the processed data (Y) being unknown. As a result, there is obtained an improved cryptographic security.

Please replace paragraph at page 1, lines 27-32 with the following amended paragraph:

~~US-A-5745577~~ U.S. Patent No. 5,745,577 discloses a method for advanced key scheduling of a secret key. The aim is to offer a protection against said mathematical attacks (differential and linear cryptanalysis) by mending the encryption algorithm. Amending the algorithm will cause

change of its output and thus the disclosed method does not present any improvement against said "Side Channel Attacks".

Please replace paragraphs at page 1, lines 34 to page 2, line 23 with the following amended paragraphs:

The present invention aims to improve the protection of a cryptographic device against "Side Channel Attacks". In short, said improvement is achieved by masking the data and/or the key by means of generating extra, auxiliary input (data or key) and compensating its influence to the output by adding, to the "main" encryption process, an auxiliary (compensating) process. By said masking measures it will be much more difficult to derive the value of data or key from the ~~behaviour~~behavior of the power consumption of the cryptographic device ~~(see page 1 lines 32-34)~~. Said masking, however, happens in such a way that the result of the ~~porcess~~process as a whole remains unchanged: with the same input and key the amended algorithm results into the same, unchanged output.

Thus the invention presents a method of the type referred to in the preamble according to the invention which is ~~characterised~~characterized by feeding, to the process, auxiliary values, while compensating, by means of an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values used in the process.

By masking the date and/or key(s) it becomes considerably more difficult to derive said values on the basis of the ~~behaviour~~behavior of the process. The result of the process, i.e., the collection of processed data, in the event of a suitable choice of the auxiliary values may be unchanged, i.e., identical to the result of the process, if no auxiliary values have been fed to it. In this connection, an "auxiliary value" is understood to mean a value (data or key) which is fed to the process as a supplement to the corresponding data and key. The invention is therefore based on the insight that the derivation of the values used in a cryptographic process is rendered considerably more difficult if said values are masked using said auxiliary values and said auxiliary process.

Please replace the paragraphs at page 2, line 34 to page 3, line 9 with the following amended paragraphs:

By deriving the key used for the known process (primary key) from a supplementary key (secondary key) using a supplementary process, there is achieved that not the (primary) key of the known process but the supplementary (secondary) key is offered to the combination of processes. In other words, externally the supplementary (secondary) key, and not the real (primary) key of the process proper, is used. Derivation of the key from the original data and the processed data has thereby become impossible. In addition, the derivation of the supplementary key has been rendered seriously more

difficult, since the combination of the original process and the supplementary process is not known.

Said embodiment of the invention is therefore based, *inter alia*, on the insight that prior knowledge of a cryptographic process is undesirable, such is contrary to what was so far assumed. Said embodiment is also based on the further insight that attacks which elaborate on knowledge of the process become considerably more difficult if the process is unknown.

The supplementary process preferably comprises a cryptographic process. This renders the derivation of the supplementary key more difficult. Basically, however, a simple encoding may be applied, e.g., as a supplementary process. In the event of a cryptographic process, there is preferably applied an auxiliary key.

The supplementary process advantageously is an invertible process. This enables the application of the method according to the invention in existing equipment with minimum modifications. If, e.g., a first device gives off a (supplementary) key which is applied in a second device according to the invention, then in the first device there may be used the inverse of the supplementary process to derive the supplementary key from the original key. In other words, although in both the first and the second device internally the original (primary) key is used, there is exchanged, between the devices, the supplementary (secondary) key. Intercepting

the supplementary key, however, does not result in knowledge of the original key.

Please replace paragraphs at page 4, lines 12 to 28 with the following amended paragraphs:

It is possible to carry out the method according to the invention in such a manner, that all primary auxiliary values are equal. As a result, a very simple practical ~~realisation~~realization is possible. The use of several auxiliary values, which are preferably random numbers and are generated anew for each time the process is carried out, however, offers a greater cryptographic security.

A further simplification of said embodiment may be obtained if the primary auxiliary values and/or secondary auxiliary values repeatedly have been combined in advance with the operation in question. This is to say, combining with auxiliary values is processed in the operation in question (e. g., a substitution), in such a manner that the result of the operation in question is equal to that of the original operation plus one or two combinatory operations with auxiliary values. By in advance including in the operation the combinatory operations, a more simple and faster practical ~~realisation~~realization is possible.

Please replace paragraph at page 6, lines 4 to 14 with the following amended paragraph:

Contrary to the situation of FIG. 1, in the situation of FIG. 2 the key K is fed to the process P from a supplementary process P*. The supplementary process P* has a supplementary (secondary) key K* as input data to produce, under the influence of an auxiliary key K', the (primary) key K as output data. The key K is therefore not fed, as is the case in the situation of FIG. 1, from an external source (e. g., a memory) to the process P, but is produced by the process P* from the supplementary (secondary) key K*:

$$K = P^*_{K'} (K^*).$$

Please replace the paragraph at page 8, lines 9 to 13 with the following amended paragraph:

By alternating the substeps of the process P, which is known per se, and the process P* (possibly known per se as well), there may be obtained a series of substeps which does not correspond to that of a known process. As a result, the nature of the process is more difficult to ~~recognise~~recognize.

Please replace paragraph at page 8, lines 36 to 42 with the following amended paragraph:

The left-hand data LD_1 and the right-hand data RD_1 of the first step S_1 were derived, in a preceding operation, from input data X and, in doing so, may undergo a preparatory processing, such as an input permutation. The output data SD_n and RD_n of the last step S_n form the processed data Y of the ~~proces~~process P, possibly after it has undergone a final operation, such as an output permutation PP^{-1}.

Please replace paragraph at page 9, lines 1 to 18 with the following amended paragraph:

The cryptographic process of FIG. 6 largely corresponds to that of FIG.5. In accordance with the invention, the data present in and between the steps is masked with auxiliary values. For this purpose, in this embodiment the first step S_1 is preceded by (preparatory) combinatory operations DC and EC, which are preferably XOR operations as well. They combine the left-hand data LD_1, and the right-hand data RD_1, respectively, which originate from the preparatory operation (PP), with a zeroth auxiliary value A_0 and a first auxiliary value A_1. The results of the combinatory operations DC and EC are left-hand masked data LD'_1 and right-hand masked data ~~RD_1~~ RD'_1, respectively (in the continuation of this text, masked data will be designated by an ~~apostrophy~~apostrophe). The maskings make themselves felt

in the subsequent steps. Since the left-hand data of the second step S_2 is equal to the masked right-hand data of the first step S_1, said left-hand data LD'_2 is masked as well. The right-hand data ~~RD_2~~ RD'_2 of the second step is masked since it is equal to the masked, modified data SD_1'.

Please replace paragraph at page 9, lines 24 to 34 with the following amended paragraph:

In order to remove the auxiliary values Ai prior to the final operation (PP^{-1}), there are provided completing combinatory operations FC and GC, which combine the modified and masked left-hand data SD'_n of the last step S_n with an auxiliary value A_{n+1} and the masked right-hand data ~~RD_n~~ RD'_n with an auxiliary value A_n, respectively. On account of Ai $\oplus$ Ai being zero in this manner the maskings are removed by the auxiliary values Ai. As a result, it is possible to carry out the method in such a manner that, notwithstanding the use of the auxiliary values A_i, the final data Y is equal to that which would have been obtained by the conventional method according to FIG. 5.

Please replace paragraphs at page 10, lines 1 to 43 with the following amended paragraphs:

There may be advantageously inserted a further combinatory operation BC_i between the cryptographic operation F_i and the combinatory operation CC_i with the purpose of combining the processed (right-hand) data FD_i

with a further (secondary) auxiliary value B_i. As a result, there may be achieved a masking of the processed data FD_i and a further masking of the (modified) left-hand data ~~SD_i~~ SD'_i. The combinatory operations AC_i and BC_i preferably are XOR operations as well.

In accordance with a further aspect of the invention, the auxiliary values Ai and Bi are related. The secondary auxiliary values Bi are formed, preferably using an XOR operation, from the first auxiliary value A_{i-1} of the previous step and the auxiliary value A_{i+1} of the next step:

$$B_i = A_{i-1} \oplus A_{i+1}$$

This results in each primary auxiliary value A_{i+1} which, using a further supplementary combinatory operation BC_i, is combined with the processed right-hand data FD_i as an ingredient of the secondary auxiliary value B_i, repeatedly being compensated in the next step, i.e., step S_{i+1}, by means of a combinatory operation AC_i before the right-hand data RD_{i+1} is subjected to the operation F_i. The (masked) right-hand data ~~RD_i~~ RD'_i in question, which forms the (masked) left-hand data ~~LD_{i+1}~~ LD'_{i+1} of the still next step S_{i+2} are combined there with the primary auxiliary value A_{i+1} and is compensated in this manner. The auxiliary value A_{i+1} makes itself felt in the modified data ~~SD_i~~ SD'_i, in such a manner that this remains masked between two steps.

The left-hand data ~~LD$_1$~~ LD'$_1$ of the first step S_1 is masked with the additional or zeroth (primary) auxiliary value A_0. By combining, with the secondary auxiliary value $B_1 = A_0 \oplus A_2$, the initial auxiliary value A_0 is removed (on account of $A_0 \oplus A_0$ being zero), but the auxiliary value A_2 and the masking achieved therewith are maintained. The zeroth auxiliary value A_0 in this embodiment is preferably chosen equal to the first auxiliary value A_1.

Although all primary auxiliary values A_i are preferably chosen to be different, with the exception of $A_0 = A_1$, it is possible to choose all primary auxiliary values A_i to be equal. In this case, all secondary auxiliary values B_i in the embodiment shown will be equal to zero, so that the further combinatory operations BC_i may be omitted. The invention further applies to processes P which contain only one step S, or have a deviating structure.

Please replace paragraph at page 11, lines 1 to 12 with the following amended paragraph:

In the process of FIG. 7, which largely corresponds to that of FIG. 6, the combinatory operations AC_i and BC_i and the cryptographic operation F_i in each step are integrated to form a combined operation ~~F_i~~ F'_i. Integrating the combinatory operations in the operations F_i is possible by suitably adjusting, e.g., a substitution table of the operation F_i. As a result, the supplementary combinatory operations AC_i and BC_i may be omitted and the result of the adjusted operation ~~F_i~~ F_i' is

equal to the result of the total of the operation F_i proper and the combinatory operations:

~~$FD_i' = F_i' (RD_i') = B_i \oplus F_i (A_i \oplus RD_i')$.~~

$FD'_i = F'_i (RD'_i) = B_i \oplus F_i (A_i \oplus RD'_i)$.

Please replace paragraph at page 11, lines 18 to 35 with the following amended paragraph:

Each time the process is carried out, the values A_i are preferably chosen anew. For the process of FIG. 7, this means that the combined operations F_i' are then determined anew. Since the operations ~~F_i'~~ F'_i in many implementations will comprise the use of several tables, such as substitution tables, said tables will be determined anew each time the process P is carried out. In order to offer a supplementary protection against attacks, according to a further aspect of the invention the tables will be determined in random order. If a combined operation ~~F_i'~~ F'_i comprises, e.g., eight tables, said eight tables will be determined in another order each time said operation ~~F_i'~~ F'_i is carried out a new. Said order may be determined on the basis of the contents of an order register, which contents may each time be formed by a random number originating from a random-number generator. On the basis of the contents of the order register there may each time be composed a fresh lookup table. Using the lookup table, the tables may be written to a memory and later be read out.

Please replace paragraphs at page 12, lines 3 to 24 with the following amended paragraphs:

The embodiment of FIG. 8 largely corresponds to that of FIG. 7. Supplementing FIG. 7, each step S_i, with the exception of the last step S_n, includes a combinatory operation HC_i which combines the right-hand data RD'_i with a tertiary auxiliary value W_i. The tertiary auxiliary value W_i preferably equals the XOR combination of the auxiliary values A_0 and A_i:

$$W = A_0 \oplus A_1,$$

where $A_0 \neq A_1$.

This results in the operation HC_i always adding the zeroth auxiliary value A_0 and compensating the first auxiliary value A_1. As a result, it is possible that all cryptographic operations F_i are essentially identical, which requires a much smaller processing and/or storage capacity from a processor system with which the method is carried out. In the embodiment of FIG. 8, the operations ~~F_i''~~ F''_i are such adjustments of the original operations F_i, that these are corrected for the auxiliary value A_1 and in addition combine the tertiary auxiliary value $W = A_0 \oplus A_1$ with their result. In other words, if $RD_i \oplus A_1$ is fed to ~~F''~~ F''_i, the result will be equal to:

~~FD_i'~~ $FD'_i = F_1(RD_1) \oplus W$.

Please replace paragraph at page 13, lines 5 to 20 with the following amended paragraph:

At the beginning of a transaction, the payment means 1 transmits an identification (card identification) ID to the payment station 2. By reference to said identification, the payment station 2 determines a key which will be used for said transaction. Said identification ID may be fed as input data X (see the figures 1-3) to a cryptographic process which, on the basis of a master key MK (not shown), produces an identification-dependent transaction key K_{ID} as output data Y. In accordance with the invention, for this purpose the process shown in the figures FIG. 2 and 3 is used, the master key MK having been converted in advance, using a process R, into a supplementary master key MK*. Said supplementary master key MK* is now fed, preferably together with the identification ID, in accordance with FIG. 3, to the supplementary process P* in order to reproduce the original master key MK and to derive the transaction key K_{ID} from the identification ID.